Subject: Electronic CIPHER, Issue 12, February 14, 1996

```
    _/_/_/_/  _/_/_/  _/_/_/_/   _/    _/  _/_/_/_/  _/_/_/_/
   _/          _/    _/     _/  _/    _/  _/        _/     _/
  _/          _/    _/_/_/_/   _/_/_/_/  _/_/      _/_/_/_/
 _/          _/    _/         _/    _/  _/        _/   _/
_/_/_/_/  _/_/_/  _/         _/    _/  _/_/_/_/  _/     _/
```

==
Newsletter of the IEEE Computer Society's TC on Security and Privacy
Electronic Issue 12   February 14, 1995   Carl Landwehr, Editor
                                   Hilarie Orman, Assoc. Editor
==

Contents: [2126 lines total]

Letter from the TC Chair

Seeing Red?

Red is the traditional color for Valentine's Day. During this last month, Internet postings involving Security and Privacy issues provoked a lot of readers to "see red".

In the wake of the Telecommunications Reform Bill (see last month's Cipher), new Internet postings continued to raise public concern over Security and Privacy on the Internet (more in this issue of Cipher). A recent incident in Maryland has generated greater interest by the legal community. A University of Maryland student posted an Internet message accusing a Maryland mother of child abuse, with the family's home telephone number. A subsequent Internet message boasted that as a result of Internet callers, the mother "had a nervous breakdown" and was "prompted to treat her daughter better". The media reports that legal experts "are investigating how to apply civil laws governing slander, libel, and invasion of privacy, as well as criminal laws governing harassment". But what about cases in which the identity of the sender is unknown and unknowable? Legal experts feel compelled to "do something", and the public appears to agree. The question is, "What"?

Still not getting Security and Privacy TC mail? We no longer keep separate membership records. All records are kept by the IEEE Computer Society. During December 1995 and January 1996, the IEEE Computer Society conducted a mail campaign to update its membership rolls. If you were missed, you can still join our TC (no fee) or update your information on-line (details in every issue of Cipher). Many of the security and privacy conferences we support are already in the planning stage, and the Computer Society will soon be mailing out registration and conference material.

We are always looking for ways to improve our TC and the services the TC provides to its members and the community. Send TC Security and Privacy correspondence to: dmcooper@ix.netcom.com.

Happy Valentine's Day!

Deborah M. Cooper
Chair, 1995-1997
IEEE Technical Committee on Security and Privacy

Letter from the Editor

Dear Readers,

It's a big issue this time, and even so there is a lot of material I have left out. The passage of the telecommunications bill with the embedded Communications Decency Act provisions has created a predictable outcry from all over the Internet. At the same time, several countries have moved to implement, or at least consider, a variety of means of controlling Internet access or content, including the U.S., France, Germany, China, and others. Since the last Cipher, Compuserve first removed access to a variety of bulletin boards and newsgroups in response to concerns voiced in Germany; but now it appears that all but a few of those sources have been reinstated.

I particularly want to express my thanks this time to Charlie Payne, Ron Ross, and Cynthia Irvine, whose reports provide an excellent account of the the Computer Security Applications Conference held in New Orleans last December. Reporting on a conference takes time both during and after the meeting, and we all benefit from the efforts of volunteers willing to take on the job. I also want to thank Hilarie Orman who continues to keep the Cipher "Calls for Papers" and Calendar columns up-to-date. Finally, thanks to Anish Mathuria for a continuing flow of items for the Cipher Reader's Guide columns.

Carl Landwehr
Editor, Cipher

SECURITY AND PRIVACY NEWS BRIEFS

Oakland Program Released; 5-minute talk abstracts due April 2

Program Co-chairs John McHugh and George Dinolt released the program for this year's Oakland symposium, which includes panels on CORBA security standards, security for medical information systems, and goals for computer security education, as well as 20 research contributions. The Symposium will again feature one session of 5-minute (rigorously enforced!) talks, in order to open the floor to new researchers, recent findings, and hot topics. Submit a one-page abstract for your five-minute talk to John McHugh, Program Co-Chair, (mchugh@cs.pdx.edu) not later than 2 April. Email submissions of 30 to 60 lines are preferred. Authors will be notified of acceptance or rejection of abstracts by April 16; accepted abstracts will be distributed at the conference. Presenters of five-minute talks are expected to register for the conference. Overtly commercial presentations are inappropriate.

Credit Cards on the Net: MasterCard, VISA Agree; First Virtual Attacks

---

[13 February 1996]
Healing an earlier split, MasterCard and Visa announced on February 1 that they have agreed on a technical standard to allow secure credit card purchases over the Internet. The specifications for the standard, called Secure Electronic Transactions (SET), are to be released in mid-February on the Visa and MasterCard web sites (http://www.visa.com) and (http://www.mastercard.com). Services based on the specification are planned to be available in late 1996. Participants in the effort with MasterCard and Visa are: GTE, IBM, Microsoft, Netscape Communications Corp., SAIC, Terisa Systems and Verisign. SET will be based on specially developed encryption technology from RSA Data Security.

As of 13 February, the specifications were not in evidence at either site. In fact, the Visa site still included a press release from June 1995 announcing that Visa and MasterCard were to cooperatively develop specifications that would be released in September 1995 leading to service in early 1996.

Perhaps anticipating the 1 February announcement, First Virtual Holdings (FVH) announced in late January that it had developed a computer program that could capture credit card numbers from unsuspecting computer users prior to any software encryption and transmit them surreptitiously to a third party via the Internet. FVH [home page: (http://fv.com/)] supports Internet electronic commerce through a scheme that avoids cryptography, transmitting a customer's credit card information via a separate telephone call. According to information released by First Virtual, the program is designed to monitor user's keystrokes, recognize sequences that appear to be credit card numbers (based on their known structure and redundancy), and transmit the numbers tracelessly across the Internet. It could be distributed as a virus or Trojan horse. Although FVH acknowledged that the elements of this attack are well known, it claimed that the synthesis of the elements was new.

Although this attack may not seem particularly innovative to Cipher readers, the announcement naturally evoked a flood of e-mail responses from people interested in cryptography generally and from those with competing commercial interests. Cipher readers interested in details from FVH's point of view should visit their web page (http://www.fv.com/ccdanger/). Olin Sibert provides a thoughtful commentary in the Risks forum, Vol. 17, Issue 69 (Feb. 7),(see URL: http://csrc.ncsl.nist.gov/rskforum/risks17.069) which seems not to have found its way into the compendium of e-mail responses available at FVH's site.

Microsoft Crypto API Project Report by Matt Blaze
[from posting to sci.crypt, 17 January, 1996]

I attended a meeting at Microsoft the other day at which they described their Crypto API project. As CAPIs go, it's reasonable enough; nothing particularly exciting about it or especially wrong with it (though they don't yet support nonblocking calls to crypto modules).

They've defined 23 cryptographic services (establish key, encrypt, etc.) that an application is expected to use for its cryptographic needs. The idea is to hide the crypto details (and keys) from applications, and to make it easy to switch from, say, wimpy

export-approved crypto to good crypto just by switching to another DLL
at load-time. The cryptography used depends on the crypto modules in
use at runtime. The API will be part of the WIN32 interface. The
next version of NT (and windows 95, I think), to be released in a few
months will support loading ``Cryptographic Service Providers'' (CSPs)
that contain the crypto functions that sit below the API. They have
(or will have soon) an application development kit to allow you to
write code that uses the API, and a CSP development kit to let you
write the crypto functions.

The interesting part is that they say they've made a deal with the
government to allow applications that use the API to be exportable as
long as they don't also try to implement crypto on their own.
Ordinarily, the government claims that ``crypto with a hole''
(applications that call a crypto API) are just as export-controlled as
crypto functions themselves, so this is something of a surprise and
would represent considerable forward progress. But, of course,
there's a catch.

The OS will not load just any old CSP. CSPs have to be signed by
Microsoft. The kernel contains a (hardcoded?) 1024 RSA public key
that it uses to check the signature when the user tries to load a CSP.
If the signature check fails, the CSP won't load. Microsoft says it
will sign any CSP from anyone AS LONG AS THEY CERTIFY THAT THEY WILL
FOLLOW THE EXPORT RULES. So you can get your CSP signed if you use
exportable cryptography or if you agree not to send it outside the US
and Canada, etc. But an end user can't just compile crypto code and
use it as a CSP, even for his or her own use, without getting it
signed by Microsoft first (actually, the CSP development kit does
allow this, but it includes a special version of the OS kernel).

I'm not sure whether this whole thing is good or bad. One important
issue is whether MS will really sign anyone's CSP or whether they will
start charging high fees or making business-based decisions on who's
CSPs they will allow (will they sign Netscape's CSP, for example).
They say they won't even look at or keep a copy of your CSP when they
sign it (at my suggestion, they are probably going to change the process
so that you send them a hash of your CSP instead of your CSP code when
you get the signature). For now they promise to sign CSPs for anyone
who returns the export certificate, at no charge. In any case,
the scheme attempts to put Microsoft, for better or for worse, in

control of the cryptography that gets used on their platforms.

We (Jack Lacy and I) will probably implement, get signed, and give away a CryptoLib-based CSP (not for export) for which we will also make source available so people can at least examine the source to the crypto they use (most CSPs will, presumably, not include source. MS plans to include an exportable RC4-40/RSA512-based "default" CSP with the OS).

Despite all this, I think it will be easy to get around the CSP signature requirements and use homebrew, unsigned crypto even with pre-compiled .exe files from other sources. I suspect it will be easy to write a program, for example, that takes an executable program and converts CryptoAPI calls to calls that look like just another DLL. And I'm sure someone will write a program to patch the NT/Windows kernel to ignore the signature check. Needless to say, it would be nice if someone outside the US were to write and distribute programs to do this. It would also be nice if someone would write a Unix/Linux version of the API/CSP mechanism. It might make it possible to export applications for those platforms as well.

I haven't tried any of this out yet, but they say they will have beta versions of the API and CSP developers kits out in a few weeks. They say that the API kit will not be export-controlled but the CSP kit will be. They plan to announce all this at the RSA conference this week.

[The 29 January issue of INFOWORLD, p. 25, reported that the Microsoft Crypto API would ship with the beta version of Windows NT 4.0 Workstation, to be shipped in the first week of February. The 22 January issue of Government Computer News reported that the NSA had awarded a contract under the MISSI program to Global Internet of Palo Alto, CA, to conduct a feasability study on how Windows NT version 3.51 might be altered to meet TCSEC B1 level requirements. The study also includes developing a prototype encryption card access control system based on Fortezza. Completion of the study is scheduled for late 1996.
-- CEL]

Case Closed on Zimmermann PGP Investigation

According to reports published in the New York Times and Wall Street

Journal, William P. Keane, an assistant U.S. Attorney in San Jose, announced on January 11 that, in consultation with the Justice Department and other administration officials, he had decided to drop the investigation of Philip Zimmermann. This means that Zimmermann will not be prosecuted for the export of PGP. Zimmermann maintained thoughout the investigation that he did not put the software on the Internet. The Internet Society's ISOC FORUM reported in its Vol. 2, No. 2, that Michael J. Yamaguchi, U.S. Attorney for the Northern District of California, announced that his office has declined prosecution of any individuals in connection with the posting to USENET in June 1991 of PGP. Both Keane and Yamaguchi have declined comment on the reasons for dropping the case and have cautioned against inferring policy decisions from these events.

IBM to provide Lotus Notes Encryption Key to U.S. Government

From the Wall Street Journal, January 18, 1996, p. B7:
IBM has agreed to provide the U.S. government with a special key that would enable government agents to more easily decode electronic messages, in exchange for permission to export a version of Lotus Notes that includes 64-bit security. The arrangement provides government officials with a key to the first 24 bits of security code, meaning that they only have to crack the remaining 40 bits to decrypt a message. U.S. Notes customers already use a 64-bit system. "We were desperate enough to try to negotiate a short-term, pragmatic solution," says Notes developer Ray Ozzie. "But we do not believe this is the right long-term solution... Our customers have been telling us that, unless we did something about the security, we could no longer call it a secure system."
[In late December 1995, Integrated Computing Engines, Inc. (ICE) of Cambridge, Mass., reported that it had cracked a 40-bit DES encryption key in less than 8 days using a single $83,000 computer. See also the following item. -- CEL]

Minimal key lengths for symmetric ciphers for commercial security

The Business Software Alliance, an industry organization devoted to preventing software piracy, hired Matt Blaze, Whitfield Diffie, Ron L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson and Michael Wiener to provide an estimate of the key lengths needed to protect commercial information under symmetric ciphers. The group's answers? "keys used to protect data today should be at least 75 bits long.

To protect information adequately for the next 20 years in the face of expected advances in computing power, keys in newly-deployed systems should be at least 90 bits long." The full report (apparently the product of a one-day meeting of the group in Chicago on November 20) is available at: <http://www.bsa.org/bsa/cryptologists.html>

Summary report on the OECD ad hoc meeting of experts on cryptography

Stewart Baker, former General Counsel of the National Security Agency and now of the law firm of Steptoe and Johnson, has written a detailed and readable account of a recent international meeting of cryptography experts and policymakers. The complete, copyrighted report is available at: <http://www.us.net/~steptoe/276908.htm> The first paragraph of the report's summary reads as follows: "The OECD's ad hoc meeting of experts on cryptography was the brainchild of U.S. policymakers. Export controls on encryption have increasingly been attacked as unworkable by U.S. software and hardware producers, who see a major market for security on the global information infrastructure. This need, they argue, will be met by foreign producers if U.S. export controls are kept in place. Many companies in the software business have also attacked the latest Administration proposal allowing the export of strong encryption only if it incorporates some form of key escrow. These companies question the international demand for key escrow."

RSA to develop crypto in China?

According to a recent Wall Street Journal report, RSA has announced a partnership with the Chinese government to fund Chinese government scientists to develop new encryption software. The software, based on RSA's algorithms, but developed in China, might be provide stronger encryption than RSA could export from the U.S. under current laws. RSA's announcement is available at <http://www.rsa.com/rsa/china_rsa.htm>

ARTICLES AND CONFERENCE REPORTS

Report on the Defensive Information Warfare Symposium, New Orleans, December 11-12 1995, by Cynthia Irvine, Naval Postgraduate School

A few years ago I watched a film about an adolescent computer whiz who broke into a sensitive military command and control system and wreaked havoc before being identified and subdued. Those were the good old days. Then hacking was an arcane art requiring a high level of technical skill and was accomplished using dumb terminal interfaces. Perhaps that scenario was never particularly realistic, but now modern hackers come in many varieties and have a vast array of tools at their disposal. Novice hackers now have at their fingertips the tools to hijack sessions, run sweepers and sniffers, perform stealth diagnostics, and engage in packet spoofing attacks. They even have nice GUIs for point and click hacking. What does this mean for the officers in charge of today's command and control system? A much greater vulnerability to attack.

On December 11 and 12, 1995, the Defense Information Security Agency/ Center for Information System Security (DISA/CISS) and the Air Intelligence Agency/Air Force Information Warfare Center (AIA/AFWIC) jointly sponsored a symposium on Defensive Information Warfare (INFOWAR). For the 200 attendees at the New Orleans meeting, the fact that several participants were called away to work on aspects of increased U.S. involvement in the Balkan region merely emphasized the increasing importance of information warfare.

Joan Pohly and her associates at DISA/CISS put together an interesting series of presentations which helped to define the problem and illustrated ongoing defensive IW efforts. Highlights of the meeting are reported here.

From the outset, it was clear that, of the services, the Air Force has made the greatest effort to address information warfare problems. The Air Force supports an impressive range of programs of which a few are: emergency response teams, automated security profiling tools, distributed intrusion detection systems, and security prototyping facilities.

So, what is ``Information Warfare?" The unclassified definition is: Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our information and information systems. In his keynote address, MG David J. Kelley, Vice Director of DISA, emphasized that information is a critical aspect of modern warfare. The battlespace presented to warfighters is dynamic and requires interoperability between systems for command and control, transmission of information, messaging, and processing. MG Kelley described how the Global Command and Control System, Defense Information System Network, Defense Message System, and Global Combat Support System will combine to provide a real time view of the combat situation with concurrent visibility of assets such as logistics, finance, and procurement. This defense information infrastructure will include air, land, and sea, as well as space-borne assets, and will require protection of critical portions of the frequency spectrum. Thus defensive information warfare specifically includes those ``measures to protect friendly information systems by preserving the availability, integrity and confidentiality of the systems and the information contained within those systems."

As emphasized by MG Kelly and subsequent speakers, including Col. Kenneth Ritchart and Sarah Jane League, both of DISA/CISS, DoD now relies on an infrastructure of networked information systems and that infrastructure is vulnerable. Not only do teenaged hackers pose a threat, but there are dangers from criminal elements, malicious insiders, those engaged in industrial and economic espionage, foreign powers, and terrorists. Highly technical powers, such as the developed nations, are particularly vulnerable to attacks on their information infrastructures. These attacks have the following attributes:

o they are low cost, in that only a few computers and network access are required to launch an attack rather than sophisticated weapons systems;
o they are low risk to the perpetrator, who can hide his tracks and/or deny illicit activity;
o a small investment can result in a high payoff in damaging an opponent's systems and provides a significant force multiplier;
o only minimal technological sophistication is needed to engage in information warfare;
o attacks can be orchestrated from anywhere at any time; and
o information warfare techniques are readily available for those with Internet access.

How does the military go after a thirteen-year-old system penetrator, and what is the legal framework in which prosecutions can be successfully mounted? Legal issues pertaining to information warfare were discussed in a talk by Col. Robert Giovagnoni of the Air Force

Office of Special Investigations. His challenge is to catch the intruder red-handed with his/her tools. Unfortunately, it is sometimes difficult to tell the normal users from the hackers until an attack is well underway and even when an attacker is identified, current legal mechanisms do not provide law enforcement with clear direction. Active defenses and hot pursuit of attackers are not usually options. For example, an attacker may be using someone else's computer as their launch point and cyberspace soldiers cannot just move in and take out an ``innocent" system. Neither do the traditional concepts of search and seizure scale well to cyberspace. Finally, Col. Giovagnoni touched on the problem of civil and criminal liability for system administrators and investigators. Often users have an expectation of privacy and, even with the use of banner pages announcing that systems are routinely monitored, only nebulous legal protections are available for system defenders.

After a thorough discussion of the nature of the defensive information warfare problem, a series of presentations described ongoing efforts to address current system vulnerabilities.

The need for continued research and development in encryption, intrusion detection, and countermeasures was the focus of session on the second day. Robin Roberts of the CIA made a particularly interesting report (though I was unable to attend it) on the agency's Workstation and Network Encryption Program. Intended to provide NSA Type-1 encryption for permanent storage and network transport in PC and LAN environments, a crypto peripheral has been developed which can be used on servers, workstations and laptops. This ongoing project gives the community a new tool with which to insert cryptographic protection with minimal disruption to ongoing operations.

The state of system accreditation was presented by Jack Eller, of CISS. Problems facing accreditations today include: overlapping accreditation responsibilities, inconsistent and incomplete policies, the high cost of accreditation, and a shift in paradigms from one in which the data owner controlled the infrastructure to one of networked systems in which the data owner no longer controls the infrastructure. The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is intended to provide a degree of standardization in the certification process while promoting methods that will reuse existing documentation and analysis and that can be applied at any stage in a system's lifecycle.

LTC Bernard Krauss presented a discussion of how DISA/CISS uses Red Teams to assess the vulnerabilities of computer systems. These assessments involve examination of the usual holes found in network operating systems. A point made during this presentation and throughout the symposium was that once an attacker has entered one system, the trust relationships between multiple systems within a network permit access to most, if not all, of the remaining systems. It is worth noting that this is the same problem encountered when one depends upon firewalls: if the interlopers can break through the firewall (or better yet find a back door into your system) they are usually free to romp around at will. Krauss emphasized that although external penetration is a threat, today the vast majority of problems are caused by insiders. Of particular interest were his slides describing the use of social engineering techniques to convince an insider to divulge sensitive information -- call up and say that General X needs the information immediately, then fool a legitimate user into reading or FAXing the data in the clear. A presentation on the INFOSEC training and awareness programs being conducted by DISA/CISS under the supervision of George Bieber provided the audience with references to resources to help insure that inside personnel understand the importance of simple security measures and precautions.

Larry Merritt, the technical director of AFWIC, told the audience that today the United States would be unable to survive a structured IW attack. During the symposium, several areas of research and development were identified. Tools to warn administrators of ongoing attacks are needed. These include automated intrusion detection systems, incident response techniques, network mapping tools to describe who is hooked up to who, near-real-time risk management tools, and techniques for rapid deployment of counter measures. The need for continuous vulnerability analysis to assess system risks was identified along with active techniques for the detection and elimination of malicious code. Tools are needed to manage interconnections to global networks. Finally enhanced training and awareness are needed to avoid trivial vulnerabilities.

Although the symposium focused on DoD, the problem of information warfare is not restricted to the defense community. DoD is becoming increasingly dependent upon the civilian information infrastructure, which is essentially world-wide. Commercial systems are no less vulnerable than their military counterparts. Perhaps this year's version of the techno-flick will be more sinister as malicious entities attack not only command and control systems, but the power grid and telephone systems as well.

Summary of the 11th Annual Computer Security Applications Conference
by Charlie Payne, Secure Computing Corporation
and Ron Ross, Institue for Defense Analyses

Sessions reported by Charlie Payne:
++++++++++++++++++++++++++++++++++++

Amid the glamour and pomp of old New Orleans, the Annual Computer Security Applications Conference (ACSAC '95) convened for its eleventh conference. Paul Strassman of SAIC was the Keynote Speaker, and Bob Courtney of Robert Courtney Company presented the Distinguished Lecture. While the conference covered many of the traditional INFOSEC topics, e.g., cryptography, database security and applications of formal methods, it was clear that securing the Internet was the hot topic, with cost-effective methods for assurance a close second.

Paul Strassman opened the conference with a call to top management to take personal responsibility for information security in their organizations. Too often, he insisted, the task is delegated to techies. Strassman advocated a security organization based on systems of governance so that there is separation of power. The executive committee is the legislative branch, while the operating management is the executive branch. Strassman stressed that only operating management, with its direct responsibility for profits, should be charged with trade-offs between security and other concerns. The judicial branch arises from the requirement that organization enforce standards. Strassman address concluded with some "bumper stickers":

o Look only to yourself for security responsibility.
o Security mismanagement is the art of making a bad situation worse.
o There is an untested presumption by everyone that they are in control.
o Any one of a thousand employees can plunge an organization into disaster.
o Never mistake for treachery what simple incompetence can explain.

Bob Courtney spoke next. He proposed that the 1996 conference committee arrange a debate between Strassman and him. He didn't elaborate on the points of disagreement; instead, he decried organizations for not understanding what they are trying protect. We're not doing a good job of defining the problem, he said, because protecting the integrity of information is a far greater problem than ensuring its confidentiality. Integrity is the property of data (or anything) "being no worse than you think it is". Access control is a poor countermeasure for protecting integrity because individuals are not held accountable. He advocated widening the internal auditor's scope to include all business processes and controls.

At the conclusion of the opening session, Marshall Abrams of The MITRE Corp. announced that "LAFS: A Logging and Auditing File System" by Christopher Wee of the University of California, Davis, won the student paper award. Later in the conference it was announced that a team of authors from the Naval Research Laboratory won the outstanding paper award with their submission, Improving Inter-Enclave Information Flow for a Secure Strike Planning Application". (postscript) The conference was presented in three tracks: two technical presentation tracks and a vendor track. The summaries below address only the technical presentation tracks that this reviewer attended.

Wednesday late morning - Track A: Firewalls

Jeremy Epstein of Cordant, Inc. introduced the three presentations: two described applications of firewall technology, while the third presentation described the secure remote control of uninterruptible power supply systems.

In "A Community of Firewalls: An Implementation Example", Dan Woycke of The MITRE Corp. described a new, firewall-based architecture for the Open Source Information System (OSIS), which is an unclassified confederation of systems serving the intelligence community. The old architecture did not support direct connection between the internal network and the Internet, and each node required strong authentication. After considering encrypting routers and managed IP service, MITRE settled on a hybrid approach: virtual private networks. The new architecture stresses usability and connectivity between nodes while retaining an acceptable level of security. It permits WWW between OSIS nodes. MITRE concludes that virtual private networks provide node-to-node connectivity and Internet connectivity while reducing the need for strong authentication.

In "Sidewinder: Combining Type Enforcement and UNIX", Dan Thomsen of Secure Computing Corp. described how Type Enforcement and other mechanisms were added to BSDi UNIX to create the company's firewall product. Four primary features were added: an administration kernel, to which there is no access from the network; an operational kernel, which enforces Type Enforcement and access to the administration kernel; triggers for detecting malicious behavior; and controlled system calls. Finally, Thomsen summarized the results of the initial Sidewinder Challenge, for which there were no successful penetration attacks.

Gerd Enste of debis Systemhaus, Germany, concluded this session with his presentation on the "Secure Remote Control and Adminstration of Uninterruptible Power Supply-Systems with SNMP". The primary threats are message modification and replay attacks. Message disclosure is not a major threat because the content of the control messages may be publicly known. Denial of service attacks are indistinguishable from ordinary network failures. The solution is a modified protocol that uses monotonic counters instead of synchronized clocks and a cryptographic algorithm for generating a message authentication code that is changed for every session or message.

Wednesday early afternoon - Track B: Forum

Steve LaFountain of NSA moderated a forum titled "Experiences Using the Common Criteria (CC) to Develop Protection Profiles (PP) and Security Targets". Forum participants were Bernard Roussely of the NATO Office of Security, Leslie LaFountain of NSA, Jon Millen of The MITRE Corp., and Ken Elliot of The Aerospace Corp. Version 1.0 of the CC will be available in January 1996, with another version appearing a year later.

Roussely described NATO's efforts to develop PPs for NATO critical systems, including a PP with C2 features (plus information labels) and B1 assurance as well as a PP for a firewall. He concluded that product PPs should be developed from system PPs, and that a method is needed to design PPs from system requirements. Roussely liked the rich database of information that appears in part 2 of the CC, but he faulted the perceived gap between a system's security objectives and the PP components. He also noted that the granularity of the components was often inappropriate.

Leslie LaFountain described NSA's goal to develop generic high and low assurance PPs for operating systems. Overall she found the CC to be very flexible and to provide useful guidance on the dependencies between features and assurance. However, the documentation requirements may be overwhelming, and some requirements, such as for assurance of modularity, are still too poorly stated.

Millen developed a PP for an application-level firewall with user authentication, access control and auditing. While most of the needed requirements were present in the CC, there was no requirement for exporting audit data. In addition, he would have liked a special interpretation of subjects and objects for clients and services, respectively, and support for different authentication mechanisms. Millen concluded that the Common Criteria needed improvement in the area of refinement.

Elliot relayed his experience developing B2-level PPs. He shared Roussely's frustration with component granularity. He also noted that the profile structure is not backward-compatible with the TCSEC. In general, the CC is still too large and too informal. However, it does provide a common language for expressing requirements, and it is flexible and extensible. Outstanding issues seem to be the unnecessary dependencies between components, the duplication of functionality and the identification of a process for profile assessment.

One audience member noted that the CC is just the TCSEC in more shades of colors; instead a PP should be something the vendor provides to make claims about what is built. Another individual noted that the utility of the CC is still unknown since only evaluators and accreditors have developed PPs.

Wednesday late afternoon - Track A: Trusted Distribution Systems
----

In the final session of the day, Emilie Siarkiewicz of Rome Laboratory moderated technical presentations on trusted distributed systems.

In "The Triad System: The Design of a Distributed, Real-Time Trusted System", John Sebes of Trusted Information Systems, Inc. described the addition of real-time features to B3 Trusted Mach (TMach). The system is so-named because it merges three areas of operating system functionality: multilevel security, real-time, and distributed processing. Triad's security functions are provided by the TMach system and by a distributed interprocess communication (IPC) mechanism for propagating security data between hosts. Real-time extensions were made to the Mach microkernel and to the TMach servers. Enforcing the security policy depends on attaching security ID tags (of the sending task) to each IPC and interpreting the tags at each node in the system. A prototype operating system has been produced. TIS believes the architecture is ideal for CORBA security.

In "Immediacy (and Consistency) in Distributed Trusted Systems", Gary Grossman of Cordant, Inc. pondered the meaning of "immediacy" for distributed systems. The term refers to the latency between the time of check and the time of use. For local systems, an action is considered "immediate" if it occurs within a bounded period, or if it occurs before some other action that could be affected by the change. However, that definition fails for distributed systems. If a security database is replicated and distributed, immediacy and consistency will conflict, and immediacy must take priority. In fact, the Trusted Network Interpretation (TNI) of the TCSEC refers to "indeterminate delays" instead of "immediacy". Grossman concludes that immediacy should only be a local system requirement, not a distributed system requirement.

Thomas Darr of CTA, Inc., concluded the session with a presentation on "Multilevel Security Issues in Real-Time Embedded Systems". He discussed the issues and problems in applying existing security technology, guidance and criteria to real-time embedded computer systems with multilevel security requirements, including finding suitable security models, identifying and characterizing the "TCB", the requirements for mandatory access controls, label mechanisms and authentication mechanisms, and the interpretation of security assurance requirements. He recommended closer ties between research and acquisition organizations and suggested further research in threat and risk-based rationales for real-time embedded system security mechanisms.

Thursday late morning - Track B: Forum

Charles Payne of Secure Computing Corp. moderated a forum titled `

"Roads to Assurance". Forum participants included Doug Landoll of Arca Systems, Inc., David Ferraiolo of NIST, Jody Heaney of The MITRE Corp, John Adams of NSA, and Jan Filsinger of Trusted Information Systems.

Landoll set the tone for the other presentations with a framework for understanding, comparing and reasoning about assurance methods. The framework, which was introduced at the 1995 Workshop on Information Technology Assurance and Trustworthiness (WITAT), considers an assurance method in three dimensions: assurance type (correctness, effectiveness, usability, workmanship), assurance source (system, process, people, environment), and assurance technique (evidence production, evidence evaluation).

Ferraiolo discussed criteria-based assurance methods, focusing primarily on the Common Criteria. The Common Criteria, whose merits were discussed earlier at this conference (see the forum above, "Experiences Using the Common Criteria to Develop Protection Profiles and Security Targets") define a set of components for expressing the assurance requirements for products and systems. The Criteria are consistent with the TCSEC (US), ITSEC (EC) and CTCPEC (Canada). In terms of Landoll's assurance framework, the Common Criteria address the correctness and effectiveness of a product or system through evidence production and evaluation.

Heaney considered the contribution of process-based methods to assurance. The two most popular methods in use, the Software Engineering Institute's Capability Maturity Model (CMM) for Software and ISO 9000, have spawned a new generation of process-based assessments, including the System Engineering CMM, the System Security Engineering CMM and the Acquisition Maturity Model. Process-based assessments not only improve the process but the product as well; however, they require significant management support. Heaney questioned whether the proposed assurance framework adequately captures process improvement and the dependencies between pieces of assurance evidence.

Adams described a recent NSA thrust to develop the Trusted Capability Maturity Model (TCMM). The TCMM model is the marriage of the CMM for Software and the Trusted Software Development Methodology (TSDM). The TSDM describes a development process for building software with a high degree of assurance that it is free from inadvertant errors or malicious code. The TCMM is a technique that yields quantitative measures of both process maturity and compliance with developmental principles that increase the trustworthiness of software. NSA's goal for the project is to replace several assessments (e.g., process-based, product-oriented, etc.) with a single assessment. The project went from ideas to results in only eight months.

Filsinger concluded the formal segment of the forum discussion with an assessment of certification and accreditation methods. C&A is unique in that it is a lifecycle assurance process, and the certifier is a consumer of the assurance evidence produced by the techniques described above. It requires claims about the operational environment and remains in effect throughout the lifecycle of the system.

An audience member noted that the success of any of these techniques still relies heavily on the pedigree of the organization. Another individual questioned why the commercial sector would ever undergo security process improvement. The answer, of course, lies in the financial reward for taking this road. Finally, someone asked if the NSA planned to combine the TCMM and the SSE-MM (both funded by NSA). Adams responded that this issue was still unresolved.

Thursday early afternoon - Track A: Intrusion Detection

Vince Reed of The MITRE Corp. moderated a technical presentation session on recent efforts in intrusion detection technology.

In "Monitoring and Controlling Suspicious Activity in Real-time With IP-Watcher", Michael Neumann of En Garde Systems described a program that allows the security administrator to monitor network logons in real-time, record only the relevant streams of data as evidence, and control the intruder by terminating or assuming control of his connection. Readers can get more information on the product at URL http://nad.infostructure.com/watcher.html.

In "Addressing Threats in World Wide Web Technology", Kraig Meyer of The Aerospace Corp. discussed threats inherent in the use of World Wide Web (WWW) technology, including disclosure, modification, fabrication and repudiation. Security services are available to address these threats at several architectural levels. None of the commercial security solutions currently being developed for Web security (e.g., SSL, SHTTP and DCE Web), however, appear to both completely address the computer security issues and be easily integrated into legacy environments.

Friday early morning - Track A: Assurance

Moderated by Marshall Abrams of The MITRE Corp., this session included presentations on the Trust Technology Assessment Program (TTAP), managing risk in software systems, and new perspectives on combining assurance evidence.

In "A New Perspective on Combining Assurance Evidence", Jay Kahn of The MITRE Corp. described an assurance evidence framework that is designed to reduce the cost of assurance while improving the chances of success for trusted system integration. The framework seeks to produce evidence that is useful, understandable, and that can be generalized and extended to provide insight into the system as a whole. The framework has three properties: it can be applied over the system lifecycle, it provides a structure for contingency planning, and it provides the ability to perform tradeoffs. It treats assurance evidence as products and focuses on their interfaces.

Friday late morning - Track A: Formal Tools

Moderated by Klaus Keus of the German Information Security Agency, this session included presentations on a method for specifying the interfaces for a C2 system, tools for developing trusted applications, and the Verification Support Environment (VSE).

In "A Semi-Formal Method for Specification of Interfaces to a C2 System", Jeremy Epstein of Cordant Inc., described a semi-formal security semantics for describing TCB interfaces. The security semantics was applied to two existing products (Novell's Netware and Cordant's Assure) to build a C2 component with over 500 TCB entry points. Using the technique, Cordant discovered many security flaws and undocumented interfaces in the underlying products; however, they were disappointed with the steep learning curve required, the difficulty of maintaining consistency between authors and with the code, and the semantics' support for testing. In retrospect, Cordant would have put more emphasis on training, and they would have based the semantics on a real programming language rather than pseudo-code. Overall the effort was worthwhile since it forced analysts and developers to understand what was security-relevant in the system, and while the effort might seem great for a C2 system, the authors felt that the semantics helped illuminate a complex discretionary access control (DAC) policy.

Sessions reported by Ron Ross
++++++++++++++++++++++++++++
Track B: Security Engineering

The session on Security Engineering, chaired by Ron Ross, Institute for Defense Analyses, presented two interesting and complementary papers in the area of security metrics and trusted software reuse. Leading off the session, Mark Aldrich, GRC Inc. presented his paper "Trusted Software, Repositories and Reuse" in which he made several observations and recommendations regarding the ability of system developers to reuse trusted software that would reside in public repositories. He provided current approaches used to identify specific components that are candidates for reuse (described as domain analysis) and described six different categories of assets that could be reused, (i.e., program source code, design specification, plans, documentation, experience and specialized expertise, and meta information about assets). The speaker then discussed the various complications introduced by sharing trusted code based on differing security policies of the systems desiring to take advantage of reuse. He concluded that reuse of components could be very beneficial if employed correctly. Special consideration must be given to ensuring that the concept of trust is not focused on a single aspect of a component such as the source code or documentation, but instead reflects a continuing thread of trust extending from the original security policy down through the machine code executing on the target system.

Following the reuse presentation, Deb Bodeau, Mitre Corporation, presented her paper, "INFOSEC Metrics: Issues and Future Directions". She began her presentation with a survey of current INFOSEC metrics, including COMPUSEC metrics, COMSEC metrics, personnel security metrics, and risk metrics. She also discussed the critical area of information valuation or the determination of asset values as part of the risk management process. She then presented the three forms of security metrics, (i.e., ranking, qualitative, and dollar equivalent) and the pros and cons of each. Building on her previous definitions and discussion, the speaker next provided some recommendations to security engineers and architects needing to use security metrics. These recommendations focused on selecting the appropriate level of abstraction for the metric, understanding the target audience, (i.e., person receiving the resulting information from the metric), and providing the correct scope for the metric. She concluded her presentation by providing several goals for INFOSEC metrics to ensure the utility of current, emerging, and new metrics. These include integrating discipline-specific INFOSEC metrics, providing common language spanning organizational boundaries, closing the gap between risk management and security engineering, and producing scalable metrics that can be targeted to systems of varying complexity.

Track B: The System Security Engineering Capability Maturity Model:
Does It Provide Appropriate System Assurance

This panel session, chaired by Rick Hefner, TRW, addressed the continuing controversial topic of using developmental assurance techniques to achieve requisite assurances about products and systems in lieu of the more traditional approaches involving system evaluation and certification. Specifically, the panel, consisting of Aaron Cohen, CSE, Milan Kuchta, CSE, John Adams, NSA, and Bill Wilson, ARCA Systems, Inc., presented position statements regarding the use of the System Security Engineering Capability Maturity Model (SSECMM) as an assurance alternative or supplement. John Adams discussed the NSA effort to develop an assurance framework which includes a variety of sources to include the SSECMM. The use of the SSECMM will provide NSA a more cost effective and timely alternative to achieving product and system assurance and facilitate the widespread use of commercial off-the shelf products. Aaron Cohen stressed the importance of developmental assurance as an alternative approach and indicated that the new Common Criteria addresses this aspect of assurance. He also stressed the need to understand the relationship among the various types of assurances and highlighted the continuing controversy within the evaluation community regarding the sufficiency of developmental assurance when applied to products. Milan Kuchta focused on understanding the specific capabilities and limitations of the SSECMM to ensure community awareness that developmental assurance will not address all aspects of assurance and trustworthiness. Bill Wilson stressed the increased sophistication and frequency of attacks on systems and that products containing only security features without appropriate assurances, are highly vulnerable to attack and easily defeated. He also talked about the benefits of organizations viewing security from a broad perspective relying on sound security analysis, from the initial requirements phase through the design, development, and implementation phases.

Track B: Access Control

This session provided an interesting contrast between role-based access control issues and a logging and auditing file system. Christopher Wee, University of California, Davis, presented his paper, "LAFS: A Logging and Auditing File System", which describes an extension to the traditional Unix-based file system with a policy-directed security logging and audit analysis for non-privileged users. LAFS allows users to specify a security policy and assists users in the configuration of file system protection mechanisms. The system also logs file accesses and audits the file access logs against the user-specified security policy. These activities are all done in a mode that is transparent to the user. The principal difference in LAFS auditing versus the more traditional auditing mechanisms is the level of granularity of the audit. LAFS limits the audit capability to files only, and does not allow any finer grain monitoring of objects within the system. The user-specified security policy is derived from a policy language that uses predicate logic and regular expressions. The language facilitates expression of Clark-Wilson style integrity policies. The speaker also described prototype implementations of the LAFS system on a variety of common platforms.

Dave Ferraiolo, National Institute of Standards and Technology, presented his paper, "Role-Based Access Control (RBAC): Features and Motivations", which began with a detailed description of the role-based access control paradigm. He discussed the central aspects of RBAC and the relationship between users, subjects, roles, objects and operations. Next, he described the notion of role hierarchies, role authorization, role activation, and separation of duty providing formal rules to specify the interaction among entities. By administratively associating access permissions with roles and making users members of those roles, the management of authorizations within the system is simplified. This provides a greater flexibility in the specification and enforcement of organizational security policies and greatly reduces the cost of security management. After a detailed presentation of the formal aspects of RBAC, the speaker stated that while certain commercial vendors have implemented RBAC features, there is still confusion within the community on precise definitions of RBAC functionality. He mentioned several research efforts that have been initiated to better define RBAC features and the capabilities and limitations of the approach.

Track A: Assurance

Julie Connolly, Mitre Corporation, presented a paper, "The Trust Technology Assessment Program and Benefits to U.S. Evaluation", in which she described the changing paradigm of trusted product evaluations. Currently, all trusted product evaluations in the U.S. are performed by the Government at the National Computer Security Center (NCSC). Under the emerging Trust Technology Assessment Program (TTAP), selected evaluations would be conducted by commercially-licensed evaluation facilities. The goals of the new program include an increase in the number of evaluated products available to the community, shorter and more timely evaluations, and the framework for mutual recognition and international reciprocity of evaluations. The speaker also described the TTAP implementation plan which initially focuses on using Trusted Computer System Evaluation Criteria (TCSEC) and an evaluation methodology based largely on the current Trusted Product Evaluation Program (TPEP). Stating the eventual goal of moving from TCSEC and TPEP to the Common Criteria and associated methodology, the speaker emphasized the need to increase the availability of commercial products and keep the focus of the commercial evaluations on lower levels of assurance. The speaker also provided a brief status report on current TTAP activities including the prototype experimental evaluation and then outlined, in detail, the expected benefits TTAP will bring to the U.S. evaluation community. These benefits included defined and consistent evaluation procedures, shorter evaluation schedules, more timely evaluations, more evaluated products, increased access to evaluations, increased vendor flexibility, and smoother transition to the Common Criteria.

Sharon Fletcher presented an interesting an informative paper entitled "Understanding and Managing Risk in Software Systems", in which she described a risk assessment methodology and toolset developed for software systems involved in safety-critical, security-critical, or mission-critical activities. The methodology introduced a framework for defining perceived risk and desired risk reduction within the context of a risk identification matrix. A system risk model captures the interactions and effectiveness of risk mitigators (or barriers) within a risk mitigators matrix. The purpose is to define an overall process for an analyst to develop a system risk model using the risk ID and mitigators matrices to guide the effort and provide essential information. Analysts perform a barrier analysis and threat analysis for each identified threat. An analysis engine determines the remaining risk within the system given the stated conditions. The model also has the ability to use cost information as part of the overall analysis effort.

COMMENTARY AND OPINION

Hacker Challenges -- Boon or Bane?
Commentary by Gene Spafford, with responses from Sameer Parekh,
Jon Wiederspan, and Jeff Weinstein

In the past year, several businesses have made resources publicly available on the Internet and challenged all comers to find bugs in them or break into them. Incentives offered to those who reported valid break-ins or bugs have ranged from T-shirts to cold cash. Recently, Gene Spafford of Purdue University decried this growing practice in a message circulated widely on the Internet. Cipher has obtained responses from some of the organizations who have sponsored challenges of one sort or another, and circulating them along with that note. We thank Prof. Spafford and the organizations who responded to our request for comments.

A Few Comments on "Hacker Challenges"
+++++++++++++++++++++++++++++++++++++++

by Eugene H. Spafford, COAST Laboratory Director, Purdue University
http://www.cs.purdue.edu/people/spaf

I note with dismay the increasing number of "hacker challenges" used in marketing security products. I think these are actually harmful to the profession and practice of security, rather than helpful. I believe the harm comes in two ways: (1) the challenges don't serve as any real test of the products, and it denigrates security professionals by suggesting that they should accept them as proof of security; and (2) it helps reinforce the image that there should be some form of reward for hacking through security measures. Neither of these are views we should responsibly seek to promote.

Consider the nature of showing the security of a product. Does a "challenge" meet the goal of testing, which is to increase one's confidence in the correct functioning of the artifact? It really doesn't, for a number of reasons:

o Few such "challenges" are conducted using established testing techniques. They are ad hoc, random tests. Thus, there is no way of determining final coverage. For instance, if 90% of all challenge attacks are of the same variety, what has the "test" really shown? (Consider testing a calculator. If you perform 10,000 tests, but 9000 of them are addition with zero, have you done a thorough job of testing?)

o That no problems are found does not mean that no problems exist. It may mean that the testers didn't expose them. Doing random, black-box testing remotely is not likely to really test much of the product. (Challenge testing is basically a form of black-box testing.)

o That no problems are reported does not mean that no problems exist. The "testers" might not have recognized them. (Look at how often software is released with bugs, even after careful scrutiny -- users don't always recognize anomalies.)

o That no problems are reported does not mean that no problems exist. How do you know that the "testers" will report what they find? How do you know the vendor is getting accurate data? If Jane Random Hacker found a way to penetrate the product in a manner that vendor monitoring didn't expose, it is possible she'd find more profitable uses (later) for that information than informing the vendor about it. Further, because of possible problems with the law, hackers might not want to report success and draw attention to themselves.

o Simply because the vendor does not report a successful penetration does not mean that one did not occur -- the vendor may choose not to report it because it would reflect poorly on its product, or not meet the narrow criteria for a "successful" penetration, or the vendor may not be able to detect it happened. (How can anyone outside prove otherwise?)

o Seldom do the really good experts, on either side of the fence, participate in such exercises. Thus, anything done is usually done by amateurs. (The "honor" of having won the challenge is not sufficient to lure the good ones into the fray. Good consultants command fees of several thousand $$ per day in some cases -- why should they donate their time and names for what amounts to free consulting and advertising?)

Also note that any such challenge also serves to aid potential hackers in their later pursuits:

- o It gives potential miscreants some period to practice breaking the system without penalty. Any other time spent hacking at one of these might result in legal action or worse. Isn't it nice the vendor is giving free practice time to the bad guys? I hope all the potential customers are equally pleased at this.
- o It gives miscreants an excuse if they are caught trying to break into the system later (e.g., "We thought the contest was still on.") This might well weaken any legal action taken later.
- o The vendor contest may actually even include some publication of hacks that don't work -- thus helping reduce the effort to compromise the system later.

Furthermore, the whole process sends the wrong message -- that we should build things and then try to break them, or that there is some prestige or glory in breaking systems. That isn't what we need. Instead, we want to promote responsible behavior, using established methods. We need to establish that security is something best done by well-trained professionals, and that hacking into systems is not "job training". (I've argued this point in more detail in "Are Computer Break-Ins Ethical?", Journal of Systems and Software, Jan 1992, 17(1).)

Good security should be carefully designed in and tested using established methods. Tiger teams have a role, but using them (especially ad hoc teams) as a major means of establishing safety is negligent. Security "contests" to demonstrate a system are worse, and should be viewed negatively by potential customers. It should be generally recognized that such contests cannot establish more than cursory confidence in a product, are not a good means of testing, and actually create a climate that may encourage or enable people to try to break the product after it is in use.

If I was a potential customer of any security product, which of the following, somewhat exaggerated approaches would be more likely to convince me that a company had its act together? Which one is the company more likely to be seeking to sell based on smoke and mirrors?

- o Approach A: Our product was coded by a bunch of really talented hackers and former system crackers who learned everything they know on the IRC. We put our product up on the Internet for 6 months, and offered a nifty backpack and some money to anyone who could break in. No one claimed the prize. Obviously, ours is a superior product.

o Approach B: Our company is certified as an ISO 9000 company. We used formal software engineering approaches to design and build our product, ending in full functional testing, D-U path testing, and statement coverage to 98%. We also hired well-known independent security experts A, B, and C under non-disclosure to examine the code and identify weaknesses, and then conduct field trials. Company X and University Y have also had the opportunity to examine and test our product, and none of them have found flaws.

Approach "B" is clearly the one we want to encourage. Approach "A" encourages cycles of "penetrate and patch" and that is what is wrong with most mass-market software available today. However, vendors claim that Approach "A" is what sells more product than Approach "B," in part because it seems to inspire more confidence, and in part because it is cheaper to produce software if they don't use an approach like "B".

If we, as a community and a profession, want better quality and more trustworthy products, we must begin to demonstrate it. The best way is in the marketplace, by showing a willingness to buy based on substance, and not flash. Saying "no" to attempts to sell us products based on "hacker challenges" is one way to do that.

Replies:
++++++++
Sameer Parekh, Community ConneXion, (sameer@c2.org
URL:http://www.c2.org/):

Most of Gene's points are very valid, and I agree with them. His points are aimed at challenges promoted by a company in order to show that a product is secure. On the other hand, the Community ConneXion challenges are promoted in order to show that a product is *insecure*.

It's easy to prove insecurity, but hard to prove security. The vendor-supported challenges are trying to prove security, which is rather misguided. In proving insecurity though, our challenges are rather simple, as they only require one counter-example to be proven that a system is insecure.
- - - - - - -

Jon Wiederspan, ComVista (jon@comvista.com URL: http://www.comvista.com/) :

We received a very similar letter from Mr. Spafford when we first began our contest and posted an extensive reply on our site while it was in operation. I will summarize the main points for Cipher readers:

1) Mr. Spafford says that these challenges are a poor way of testing software. That is true, however it was never our purpose to test the software by running a challenge. The testing has been completed or we would not have been confident enough to place $10,000 on the line. The main purpose of our security challenge was to promote awareness of the existence of security options for Macintosh servers. It was never intended as proof of the security of the system or to replace rigorous testing.

2) Mr. Spafford says that these contests promote hacking. We disagree with that entirely. By his argument, the Daytona 500 is responsible for people driving too fast on highways. I think there are people who drive as if they are on a race track (one passed me this morning on my way to work) but it is clear that rules on the highway are different from rules on the race track and no court in the land would let a person get away with arguing differently. We clearly stated on our site the limitations of the contest including a warning that we were not condoning similar attacks on systems other than the one provided for the contest.

3) Mr. Spafford says that these contests make it easier to break other systems. Mr. Spafford is looking in the wrong place. Bulletin boards, newsletters, Web sites and more all exist with information on how to hack into systems. Books have been written on the subject, movies made, and special investigative reports offered on television all on the subject. Writing about what failed on our site will not help hackers significantly. Our site also did not provide free practice to hackers because *none of the attempts worked*. Practice is useless if you do not at some point succeed.

4) Mr. Spafford says that it is wrong to test things by trying to break them. I don't think he thought about what he was saying there. What is beta testing but an attempt to find where software will break? Stress testing for metal structures? Crash testing cars? It is a fact of life

that part of testing a product is to find where it will fail, which means trying actively to break the product in a variety of ways.

In summary, it is our opinion that Mr. Spafford's letter has no bearing on the challenge that we had online. He probably would have been better served by investigating our site more thoroughly before writing the letter.

- - - - - -

Jeff Weinstein, Netscape (jsw@netscape.com, URL: http://home.netscape.com/people/jsw)

My quick reaction is that the Netscape Bugs Bounty is not a "hacker challenge". It is a way to reward users for helping to find bugs that get past us. I don't think that we make any claims such as "our product must be secure because no one claimed our hacker prize". We also don't view the bug bounty as a replacement for our own QA efforts, but a supplement to it.

- - - - - -

Secure Computing Corporation, sponsors of the Sidewinder challenge reported in Cipher EI#6, declined to comment.

New Reports available via FTP and WWW

An experience teaching a graduate course in cryptography by Avi Rubin,
Available at URL: <ftp://thumper.bellcore.com/pub/rubin/fall95.ps.Z>

Papers from WWW4, Fourth International World Wide Web Conference
WWW4, Fourth International World Wide Web Conference ``The Web Revolution"
December 11-14, 1995, Boston, Massachusetts, USA:

Low Level Security in Java, by Frank Yellin
<http://www.w3.org/pub/Conferences/WWW4/Papers/197/40.html>

CCI-Based Web Security: A Design Using PGP, by Judson D. Weeks, Adam Cain,
Briand Sanderson
<http://www.w3.org/pub/Conferences/WWW4/Papers2/245.html>

Securing the World Wide Web: Smart Tokens and Their Implementation,
by Michael F. Jones, Bruce Schneier
<http://www.w3.org/pub/Conferences/WWW4/Papers/330/>

Scalable, Secure, Cash Payment for WWW Resources with the PayMe Protocol
Set, by Michael Peirce, Donal O'Mahony
<http://www.w3.org/pub/Conferences/WWW4/Papers/228/>

The Millicent Protocol for Inexpensive Electronic Commerce, by Steve
Glassman, Mark Manasse, Martin Abadi, Paul Gauthier, Patrick Sobalvarro
<http://www.w3.org/pub/Conferences/WWW4/Papers/246/>

Dorothy Denning on the future of cryptography and "crypto anarchy"
<http://www.cosc.georgetown.edu/~denning/crypto/Future.html>

PC Week article comparing network security scanners, 5 Feb. 1996
<http://www.zdnet.com/~pcweek/netweek/0205/tdaem.html>

Papers and information on SKIP - Simple Key management for Internet
Protocols. Includes pointers to papers and recent Internet Drafts
<http://skip.incog.com/>

Internet Drafts:

The Secure HyperText Transfer Protocol, by E. Rescorla and A.
Schiffman. Revised 2/13/96. 47 pages.
<http://ds.internic.net/internet-drafts/draft-ietf-wts-shttp-01.txt>
This memo describes a syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. Secure HTTP (S-HTTP) is an extension of HTTP, providing independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin.

Security Extensions for HTML, by E. Rescorla and A. Schiffman.
2/13/97. 3 pages.
<http://ds.internic.net/internet-drafts/draft-ietf-wts-shtml-00.txt>
This memo describes a syntax for embedding S-HTTP negotiation parameters in HTML documents. S-HTTP as described by draft-ietf-wts-shttp-01.txt contains the concept of negotation headers which reflect the potential receiver of a message's preferences as to which cryptographic enhancements should be applied to the message. This document describes a syntax for binding these negotiation parameters to HTML anchors.

A Proposed Extension to HTTP : Digest Access Authentication,
by J. Hostetler, J. Franks, P. Hallam-Baker, A. Luotonen, E. Sink,
L. Stewart. Internet Draft, dated 20 December 1995.

<http://ds.internic.net/internet-drafts/draft-ietf-http-digest-aa-02.txt>
The protocol referred to as "HTTP/1.0" includes specification for a Basic Access Authentication scheme. This scheme is not considered to be a secure method of user authentication, as the user name and password are passed over the network in an unencrypted form. A specification for a new authentication scheme is needed for future versions of the HTTP protocol. This document provides specification for such a scheme, referred to as "Digest Access Authentication". The encryption method used is the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Interesting Links [new entries only]

Format:
Description (first lines) followed by URL (last line)

Government sources/information:

[no new entries]

Professional societies and organizations:

Technical Council on Software Engineering (IEEE Computer Society)
<http://www.tcse.org>

Other places for interesting research papers, announcements, assistance
----
Fred Cohen's "Infosec Heaven"
<http://all.net/heaven.html>

Who's Where: recent address changes

Entered 12 February 1996:

Cristi Garvey
Director Server Software Development
Illustra Information Technologies, Inc.
1111 Broadway
Suite 2000
Oakland, CA 94607
voice: (510)873-6226

fax: (510)869-6388
e-mail: cristi@illustra.com
home page: http://www.illustra.com

Calls for Papers (new listings since last issue only -- full list on Web)

(see also Calendar)
CONFERENCES

Listed earliest deadline first. See also Cipher Calendar and NRL CHACS CFP list.

o National Information Systems Security Conference, Baltimore, Maryland, October 22-25, 1996. The National Information Systems Security Conference audience represents a broad range of information security interests spanning government, industry, commercial, and academic communities. The committee especially encourages student papers written by individuals in degree programs. The student should not have been previously published, and the paper shall be endorsed by an academic advisor. Eight paper copies of papers or panel proposals are by February 16, 1996, to the address in the announcement. Queries to: NISSConference@Dockmaster.ncsc.mil.

o Communications and Multimedia Security Communications and Multimedia Security, University of Essen, Germany, September 23- 24, 1996. Joint Working Conference IFIP TC-6 and TC-11. Several security topics in this area are of interest. Contributions written in English shall not exceed 6000 words. Eight copies of the paper should be submitted to Prof. Dr. Patrick Horster, University of Chemnitz by March 1, 1996. Electronic submissions can't be accepted. The proceedings shall be published by an international publisher.

o Mobile Computing and Networking 1996, Rye, NY, November 11-12, 1996. Original papers of no more than 15 pages are solicited. Papers of particular merit will be selected for publication in the ACM/Baltzer Journal on Wireless Networks and the ACM/Baltzer Mobile Networks & Nomadic Applications Journal. A topic of interest is: Security, scalability and reliability issues for mobile/wireless systems. Electronic submissions of postscript to mobicom96@gucci.mirc.gatech.edu are due by March 1, 1996. Web page: <http://www.info.acm.org/sigcomm/mobicomm96>.

o International Workshop on Enterprise Security, Stanford University, California, June 19-21, 1996. This workshop is aiming to bring together principal players in the Enterprise Security; including the Internet; to discuss the problems and challenges of security. Papers, panels, and position papers are sought. Papers are due by March 15, 1996. Mail six copies of an original (not submitted or published elsewhere) paper (double-spaced) of 3000-5000 words to the Program Chair. Include the title of the paper, the name and affiliation of each author, a 150-word abstract and no more than 8 keywords. The name, position, address, telephone number, and if possible, fax number and e-mail address of the author responsible for correspondence of the paper must be included.
Web page <http://www.cerc.wvu.edu/SECWK>

o Invitational Workshop on Computer Vulnerability Data Sharing, Gaithersburg, MD, June 10-12, 1996. Researchers in communities including intrusion detection, security, incident handling, and software engineering have long expressed an interest in having access to a repository of vulnerability data that could be used in their experiments and analyses. These communities have different requirements for such a repository and would derive different benefits from it. These differences have often been cited as obstacles to the creation or sharing of such a repository. The purpose of this invitational workshop is to bring together interested researchers from these communities to explore these differences and questions. We hope to reach a consensus on creating a repository that can benefit all. Individuals interested in attending the workshop are invited to submit a position paper draft to the program committee. Invitations will be extended by the program committee based on these drafts. Extended abstracts (PostScript or ASCII test due March 8 via e-mail to vuln_workshop@cs.purdue.edu. Invitations extended April 10, final papers (20 pages maximum) due May 8. For full call for papers send e-mail to workshop-cfp@cs.purdue.edu or browse Web page <http://www.cs.purdue.edu/coast/workshop.ps>

o Multi-Media Database Management Systems, Mountain Lake, NY, August 14-16, 1996. Access Security Issues is a topic of interest for the conference. Authors are invited to submit 4 copies of each paper not exceeding 25 double-spaced pages, including figures, pictures,

etc. to Dr. Kingsley C. Nwosu by March 15, 1996.
Web page: <http://drum.ncsc.org/~nwosuck/iwmmdbms96.html>

o Integration of Enterprise Information and Processes: Rethinking Documents. Cambridge, Massachusetts, November 14, 1996. Managing enterprise information offers opportunities for new forms of security controls, especially when large scale intra and inter-company collaborations are involved. This conference focuses on integration of enterprise information, including process and workflow models. Authors are invited to submit extended abstracts (one to two single-spaced pages) via email to ipic96@iti.gov.sg by March 18th 1996.
Web page: <http://www.iti.gov.sg/conference/ipic96.html>

o Advanced Transaction Models and Architectures, Goa, India, August 31 - September 2, 1996. The committee solicits papers describing original ideas and new results on the foundations, applications, and development of transaction systems. Transactions in multilevel secure database systems is a topic of interest. Submissions from USA are due to Sushil Jajodia (jajodia@isse.gmu.edu) by March 31, 1996. Authors are invited to submit six copies of papers. The text must be submitted in English. Papers should be limited to 6000 words, full page figures being counted as 300 words. Each paper must include a short abstract and a list of keywords indicating subject classification.
Web page: <http://www.neward.rutgers.edu/~atluri/atma.html>

o New Security Paradigms '96, Lake Arrowhead, Cal., Sept. 16-19, 1996. This workshop explores radical new models for computer security, such as strategies for securing very large networks, providing software safety in large systems, and developing ethics in international cyberspace. To participate, submit either a research paper or a 5-10 page position paper, preferably via email, to Program Chairs Catherine Meadows (Meadows@itd.nrl.navy.mil) and David Bailey (daveb@gcsi.com) by April 1, 1996. Alternately, submit five copies of a hard-copy paper to either program chair by March 24, 1996.
Web page: <http://www.itd.nrl.navy.mil/ITD/5540/acm/new-paradigms.html>

o Theorem Proving in Higher Order Logics, Turku, Finland, 27-30 August 1996. The programme committee welcome submissions on all aspects of theorem proving, particularly those relating to higher order logics or to proof systems based on secure mechanizations of logic.

Submissions of full research papers are due via email to orgcom@abo.fi by 15 March 1996; informal research reports are due by April 14.
Web page: <http://www.abo.fi/~jharriso/TPHOLs96.html>

o Operating Systems Design and Implementation '96, Seattle, Washington, October 29, 1996 - November 1, 1996. The OSDI Symposium emphasizes both innovative research and quantified experience in operating systems. Security in distributed systems is one topic of interest. Full papers are due by May 7, 1996; fifteen paper copies of a submission no more than 14 pages long should be sent to Willy Zwaenepoel, Department of Computer Science, Rice University, 6100 S. Main St., Houston, TX 77005, USA. A postscript copy should be sent via email to osdi-papers@cs.rice.edu.

o ASIACRYPT '96, Kyongju, South Korea, November 3-7, 1996. Authors are invited to submit original papers, neither published nor submitted for publication elsewhere, by sending 16 copies of an extended abstract containing at most 10 single-spaced pages of 12pt type, not counting the bibliography and clearly marked appendices to Dr. Kwangjo Kim by May 20, 1996.
Web page: <http://www.kreonet.re.kr/AC/AC96.html>

o Dependable Computing for Critical Applications, Partenkirchen, Germany, March 5-7, 1997. Papers are sought in all areas of dependable computing, including but not limited to models, methods, algorithms, tools and practical experience with specifying, designing, implementing, assessing, validating, operating, and maintaining dependable computing systems. Papers that deal with man-machine interface issues (as they relate to dependability) are specifically encouraged. Of particular but not exclusive interest will be presentations that address combinations of dependability attributes, e.g., safety and security, through studies of either a theoretical or an applied nature. Submissions via mail by September 3, 1996.

JOURNALS

Regular archival computer security journals:

o Journal of Computer Security (JCS) [see Cipher Web pages or EI#9]; e-mail contacts for submissions: jajodia@isse.gmu.edu or jkm@mitre.org

o Computers & Security [see Cipher Web pages or EI#9]
e-mail contact for submissions: j.meyer@elsevier.co.uk

Special Issues of Journals and Handbooks: listed earliest deadline first.

[No new entries this issue]

Reader's Guide to Current Technical Literature in Security and Privacy
Part 1: Conference Papers

1996 IEEE S&P, 1995 IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 6-8, 1996

- An Analysis of the Timed Z-Channel; Ira S. Moskowitz, Steven J. Greenwald, Myong H. Kang
- Defining Noninterference in the Temporal Logic of Actions; Todd Fine
- Security for Medical Information Systems; Ross Anderson
- Entity Authentication; Dieter Gollmann
- A Fair Non-repudiation Protocol; Jianying Zhou, Dieter Gollmann
- Limitations on Design Principles for Public Key Protocols; Paul Syverson
- Ensuring Atomicity of Multilevel Transactions; Paul Ammann, Sushil Jajodia, Indrakshi Ray
- View-Based Access Control with High Assurance; Xiaolei Qian
- Supporting Multiple Access Control Policies in Database Systems; Elisa Bertino, Sushil Jajodia, Pierangela Samarati
- An Immunological Approach to Change Detection: Algorithms, Analysis, and Implications; Patrik D'Haeseleer, Stephanie Forrest, Paul Helman
- A Sense of Self for UNIX Processes; Stephanie Forrest, Steven A. Hofmeyr, Anil Somayaji, Thomas A. Longstaff
- Cryptovirology: Extortion Based Security Threats and Countermeasures; Adam Young, Moti Yung
- A Security Model of Dynamic Labeling Providing a Tiered Approach to Verification; Simon Foley, Li Gong, Xiaolei Qian
- A Communication Agreement Framework of Access Control; Martin Roscheisen, Terry Winograd
- Decentralized Trust Management; Matt Blaze, Joan Feigenbaum, Jack Lacy
- Security Properties and CSP; Steve Schneider
- Security Flaws in the HotJava Web Browser; Drew Dean, Dan S. Wallach
- On Two Proposals for On-line Credit-card Payments using Open Networks: Problems and Solutions; Wenbo Mao
- Secure Network Objects; Leendert van Doorn, Martin Abadi, Mike Burrows, Edward Wobber
- Run-Time Security Evaluation (RTSE) for Distributed Applications; Cristina Serban, B. McMillin

IDMS'96, European Workshop on Interactive Distributed Multimedia Systems
and Services, March 4-6, 1996, Berlin, Germany (security-related papers):
 - A Secure Architecture for Tenet Scheme 2; R. Oppliger (Univ. of Berne,
   Switzerland), A. Gupta, M. Moran (ICSI, USA), R. Bettati (Texas A&M, USA)
 - The Secure Conferencing User Agent: A Tool to Provide Secure
   Conferencing with MBone Multimedia Conferencing Applications
   E. Hinsch, A. Jaegermann, L. Wang (GMD TKT, Germany), I.C. Roper
   (Univ. of Plymouth, UK)
ICDP'96, IFIP/IEEE International Conference on Distributed Platforms,
Feb 27 - March 1, 1996, Dresden, Germany (security-related paper only):
 - Security Architecture based on Secret Key and Privilege Attribute
   Certificates, Y. Sameshima (Hitachi Software Engineering Co., Japan)
IEEE COMPCON '96, Feb. 25-28, 1996, Santa Clara, CA (security-related
   paper only):
 - Mobile Agent Security and Telescript, J. Tardo and L. Valente
   (General Magic Inc, USA)
NETWORKS'96, IASTED International Conference, January 8-10, 1996,
Orlando, Florida, USA (security-related papers only);
 - An Access Determination Algorithm for Preventing Non-secure Information
   Flows; Y. Oki, T. Shimomura, T. Ohta (Japan)
 - Secure Communication Services in the Masix Distributed Operating System;
   J. Simon, F. Mevel (France)
 - Message Delivery Certification Scheme based on the Fiat-Shamir
   Identification Scheme; M. Kanda, Y. Takashima, K. Yamanaka (Japan)
 - Network Security Scheme Based on Error Correcting Codes; Y.I. Kang,
   S.H. Yoon, T.Y. Kim (Korea)
 - A High-Speed DES Implementation using Temporal Parallelism; T.-K. Park,
   D.-J. Hwang (Korea)
ACSC'96, Nineteenth Australasian Computer Science Conference, 31 January -
2 February 1996, Melbourne, Australia (security-related papers only):
  - Analysis of a Key Distribution Protocol for a Secure LAN-SMDS
    Network V. Varadharajan, C. Calvelli
  - A Combinatorial Pattern Matching Problem with Applications to
    Cryptography J. Golic, L. O'Connor
  - Smart Card Integration with Kerberos M. Warner, J. Trinkle, G. Gaskell
  - Language Mechanisms for Protecting Persistent Data M. Hollins, J.
    Rosenberg, M. Hitchens
WWW4, Fourth International World Wide Web Conference, "The Web
Revolution", December 11-14, 1995, Boston, Massachusetts, USA
   (security-related papers only)
 - Low Level Security in Java; Frank Yellin

- CCI-Based Web Security: A Design Using PGP; Judson D. Weeks, Adam Cain, Briand Sanderson
- Securing the World Wide Web: Smart Tokens and Their Implementation; Michael F. Jones, Bruce Schneier
- Scalable, Secure, Cash Payment for WWW Resources with the PayMe Protocol Set; Michael Peirce, Donal O'Mahony
- The Millicent Protocol for Inexpensive Electronic Commerce; Steve Glassman, Mark Manasse, Martin Abadi, Paul Gauthier, Patrick Sobalvarro

---

Reader's Guide to Current Technical Literature in Security and Privacy
Part 2: Journal and Newsletter Articles, Book Chapters

---

* ACM SIGSAC Security Audit & Control Review, Vol. 14, No. 1 (January 1996).
 - Report from New Security Paradigms Workshop. pp.2-3.
 - V. K. Murthy. Probabilistic Quorum Protocols for Biometrical User Authentication in OLTP. pp. 5-10.
* IEEE Transactions on Software Engineering, Vol. 22, No. 1 (January 1996), Special Section -- Best Papers of the IEEE Symposium on Security and Privacy 1994:
 - J. McHugh. Guest Editorial: Introduction to the special section. pp. 3-5.
 - M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. pp. 6-15.
 - N. Heintze and J. D. Tygar. A model for secure protocols and their compositions. pp.16-30.
 - M. K. Reiter. A secure group membership protocol. pp. 31-42.
 - J. McLean. A general theory of composition for a class of "possibilistic" properties. pp. 53-67.
* IEEE Transactions on Computers, Vol. 45, No. 1 (January 1996): J. Dj. Golic. Linear models for keystream generators. pp. 41-49.
* Distributed Computing, Vol. 9, No. 3 (1995): L. Gong. Efficient network authentication protocols: lower bounds and optimal implementations. pp. 131-145.
* Scientific American, Vol. 273, No. 6 (December 1995): T. Beth. Confidential communication on the Internet. pp. 270-273.
* Information Processing Letters, Vol. 57, No. 1 (January 1996): W-B. Lee and C-C. Chang. Integrating authentication in public key distribution system. pp. 49-52.
* Computers & Security Volume 14, Number 8 (1995). (Elsevier) Refereed Papers:
 - Love Ekenberg, Subhash Oberoi, and Istvan Orci. A cost model for managing information security hazards. pp. 707-718.
 - Marshall Abrams and Marvin Zelkowitz. Striving for correctness. pp. 719-738.

* Computers & Security Volume 14, Number 7 (1995). (Elsevier) Refereed Papers:
 - B.C. Soh and T. S. Dillon. Setting optimal intrusion-detecton thresholds.
   pp. 621-632.
 - W. Fred de Koning. A methodology for the design of security plans. pp.
   633-644.
 - James Backhouse and Gurpreet Dhillon. Corporate computer crime management:
   a research perspective. pp. 645-652.
* IEEE Spectrum, Vol. 32, No. 12 (December 1995). J. Adam. The privacy problem.
  pp. 46-52.
* Information Processing Letters, Vol. 56, No. 5 (December 1995): A.M.
  Youssef and S.E. Tavares. Resistance of balanced s-boxes to linear and
  differential cryptanalysis. pp. 249-252.
* IEEE Personal Communications, Vol. 2, No. 5 (October 1995): D. Chess,
  B. Grosof, C. Harrison, D. Levine, C. Parris and G. Tsudik. Itinerant
  Agents for Mobile Computing. pp. 34-49.
* ACM SIGAPP Applied Computing Review, Vol. 3, No. 1 (Summer 1995).
  Special Issue on Security, B. Unger, Guest Editor:
 - C. Angaye. Security in a Networked Environment. pp. 2-5.
 - R. Li and E. Unger. Security Issues with TCP/IP. pp. 6-13.
 - S. Hansen. Hybrid Inferential Security Methods for Statistical Databases.
   pp. 14-18.

Reader's Guide to Current Technical Literature in Security and Privacy
Part 3: Books

It's not exactly technical literature, but three recently released books on the latest pursuit and apprehension of Kevin Mitnick are attracting considerable attention:

 - Tsutomu Shimomura and John Markoff. Takedown. Hyperion, 324 pp., $24.95.
   The pursuit and capture of Kevin Mitnick.
 - Jonathan Littman. The Fugitive Game. Little, Brown & Co., 383 pp., $23.95.
 - Jeff Goodell. The Cyberthief and the Samurai. Dell. $5.99.

For a review by James Fallows covering all three, see New York Times Book Review, Feb. 4, 1996, p. 14. Coverage of the first two can also be found in The New Yorker, Jan. 30, 1996.

Calendar

Internet Conference Calendar, URL:http://www.automatrix.com/conferences/ is also worth a look.

```
Dates       Event, Location    Point of Contact/ more information
-----      ---------------    ----------------------------------
==========================================================================
See Calls for Papers section for details on many of these listings.
==========================================================================
 o 2/14/96: CRYPTO96. Santa Barbara, CA. Submissions due to
         koblitz@math.washington.edu
 o 2/16/96: NISS96, Baltimore, Maryland. Paper submissions due by mail
 o 2/20/96: IFIP WG 11.3, Como, Italy, submissions due, samarati@dsi.unimi.it or
         sandhu@isse.gmu.edu
 o 2/20/96- 2/21/96: FISP96, San Diego, CA; Federal Internet Security Plan
 o 2/21/96- 2/23/96: FSE Workshop '96, Cambridge, UK, dieter@dcs.rhbnc.ac.uk
 o 2/21/96: Secure Email Wkshp, San Jose CA. Registration
 o 2/22/96- 2/23/96: SNDSS '96, San Diego, CA
 o 2/23/96: VLDB96, Bombay, India. American submissions due
         mohan@almaden.ibm.com
 o 2/26/96- 3/ 1/96: ICDE '96, New Orleans; icde96@cis.ufl.edu
 o 2/26/96- 2/27/96: IMC'96, Rostock, Germany
 o 3/ 1/96: WebNet. San Francisco, CA; Submissions to AACE@virginia.edu
 o 3/ 1/96: SCRAPC96, Lille, France . Submissions due by mail
 o 3/ 1/96: IFIPTC6TC11, U of Essen, Germany;  hard-copy submissions due
 o 3/ 1/96: MOBICOM '96, Rye, NY; Email submissions due to
         mobicom96@gucci.mirc.gatech.edu
 o 3/ 5/97- 3/ 7/97: DCCA6. Partenkirchen, Germany. Submissions due by mail
 o 3/ 7/96- 3/ 8/96: RTDB96, Newport Beach, California.
 o 3/ 8/96: NIST Invitational Workshop on Vulnerability Data Sharing
         abstracts due to vuln_workshop@cs.purdue.edu
 o 3/14/96- 3/16/96: CCS-3, New Delhi; gong@csl.sri.com or
         Jacques.Stern@ens.fr
 o 3/15/96: ESORICS'96, Rome, Italy. Submissions due;
         bertino@hermes.mc.dsi.unimi.it
 o 3/15/96: HASE96. Niagara-on-the-Lake, Canada Hard-copy
         submissions due to sourav@acm.org
 o 3/15/96: IWES, Stanford University, California; Hardcopy
         submissions due to program chair
 o 3/15/96: PRAGOCRYPT '96, Prague. Papers due by mail
 o 3/15/96: MMDMS, Mountain Lake, NY. Submissions due by mail
 o 3/15/96: TPHOLs '96, Turku, Finland;
 o 3/18/96: KDD96. Portland, Oregon; Submissions due, kdd@aaai.org.
 o 3/18/96: IPIC96, Cambridge, Massachusetts; Submissions due
         to ipic96@iti.gov.sg
```

```
o 3/18/96- 3/22/96: FME '96, Oxford University, England
o 3/19/96: USENIX Sec Symp, San Jose, California; Abstracts
        due, details from securityauthors@usenix.org
o 3/21/96- 3/24/96: TSMCFP96 Nashville, Tenn.; lundeng@ctrvax.vanderbilt.edu.
o 3/27/96- 3/30/96: CFP '96, Cambridge, MA; cfp96@mit.edu
o 3/31/96: ATMA, Goa, India; Papers (from USA) due to Sushil Jajodia
o 3/31/96: DEXA96. Zurich, Switzerland; Submissions due;
        dexa@faw.uni-linz.ac.at for info
o 4/ 1/96: NSP '96: submissions due to meadows@itd.nrl.navy.mil and
        daveb@gcsi.com;
o 4/10/96- 4/13/96: CWCP, Cambridge, UK; tmal@cl.cam.ac.uk
o 4/16/96- 4/18/96: METAD. Silver Spring, Maryland
o 4/30/96- 5/ 3/96: 8th CCSS, Ottawa; questions to ccss96@cse.dnd.ca.
o 5/ 5/96- 5/ 8/96: IEEE S&P 96; dmj@mitre.org
o 5/ 6/96- 5/11/96: WWWC96, Paris, France,
o 5/ 7/96: OSDI '96 Seattle, WA. Paper submissions due by mail and email to
        osdi-papers@cs.rice.edu
o 5/20/96: ASIACRYPT96 Kyongju, South Korea; Paper submissions due by mail
o 5/21/96- 5/24/96: IFIP/SEC 96 - Greece; sec96@aegean.ariadne-t.gr
o 5/27/96- 5/30/96: ICDCS96 Kowloon, Hong Kong.
o 5/30/96- 6/1/96: IH Workshop '96, Cambridge, UK; ross.anderson@cl.cam.ac.uk
o 6/ 2/96: DMKD96 Montreal, Canada. Web page
o 6/ 3/96- 6/ 6/96: SIGMOD/PODS '96, Montreal, Canada
o 6/ 3/96- 6/ 5/96: SOC18, Kingston, Ontario, Canada.
o 6/ 4/96- 6/ 6/96: SECURICOM '96, Paris, France.
o 6/ 7/96: SAC '96, Kingston, Ontario, Canada. Submissions due via mail
o 6/10/96- 6/12/96: CSFW96. County Kerry, Ireland Wkshop Web page.
o 6/10/96- 6/11/96: ISTCS96. Jerusalem, Israel.
o 6/10/96- 6/12/96: NIST Invitational Workshop on Vulnerability Data Sharing
                Gaithersburg, MD
o 6/12/96- 6/14/96: BDBIS. Tallinn, Estonia
o 6/17/96- 6/21/96: COMPASS96, Gaithersburg, Maryland;
o 6/13/96: ICDT97, Delphi, Greece; Submissions due to afrati@cs.ece.ntua.gr
o 6/18/96- 6/20/96: ICSSDBM '96, Stockholm; pers@sto.foa.se
o 6/19/96- 6/21/96: CoopIS96, Brussels, Belgium. .
o 6/19/96- 6/21/96: IWES. Stanford University, California
o 6/24/96- 6/26/96: ACISP96, Woolongong, NSW, Australia.
o 6/25/96- 6/28/96: INET96. Montreal, Canada
o 7/22/96- 7/24/96: IFIP WG 11.3, Como, Italy, samarati@dsi.unimi.it or
                 sandhu@isse.gmu.edu
o 7/22/96- 7/25/96: USENIX Sec Symp, San Jose, California;
```

o 8/ 3/96- 8/ 5/96: KDD96. Portland, Oregon See Web page.
o 8/14/96- 8/16/96: MMDMS, Mountain Lake, NY.
o 8/15/96- 8/16/96: SAC '96, Kingston, Ontario, Canada
o 8/18/96- 8/22/96: CRYPTO96, Santa Barbara, California
o 8/27/96- 8/30/96: TPHOLs '96, Turku, Finland;
o 8/31/96- 9/ 2/96: ATMA, Goa, India;
o 9/2/96-9/6/96: IFIP96 Mobile Commns Canberra, Australia.
o 9/ 3/96- 9/ 6/96: VLDB96, Bombay, India
o 9/ 3/96: DCCA6, Partenkirchen, Germany.
o 9/ 9/96- 9/13/96: DEXA96, Zurich, Switzerland.
o 9/16/96 - 9/19/96: NSP '96, Lake Arrowhead, CA ; questions to
newparadigms96@itd.nrl.navy.mil.
o 9/18/96- 9/20/96: SCRAPC96, Lille, France
o 9/23/96- 9/24/96: IFIPTC6TC11, University of Essen, Germany;
o 9/23/96- 9/27/96: SDSP96, Perth, Australia
o 9/25/96- 9/27/96: ESORICS'96, Rome; bertino@hermes.mc.dsi.unimi.it
o 9/30/96-10/ 3/96: PRAGOCRYPT '96, Prague
o 10/16/96-10/19/96: WebNet. San Francisco, CA
o 11/ 3/96-11/ 7/96: ASIACRYPT96, Kyongju, South Korea
o 11/11/96-11/12/96: MOBICOM96, Rye, NY;
o 11/14/96-11/15/96: IPIC96, Cambridge, Massachusetts;
o 10/22/96: HASE96. Niagara-on-the-Lake, Canada;
o 10/22/96-10/25/96: NISS96. Baltimore, Maryland
o 10/29/96-11/ 1/96: OSDI '96 Seattle, WA.
o 11/??/96: ESORICS '96, Rome, Italy; no e-mail address available
o 1/ 8/97- 1/10/97: ICDT97, Delphi, Greece;
o 2/??/97: PAKDD '97, Singapore. Info hweeleng@iti.gov.sg;
o 5/ 4/97- 5/ 7/97: IEEE S&P 97; no e-mail address available
o 5/13/97- 5/16/97: 9th CCSS, Ottawa; no e-mail address available
o 5/ 3/98- 5/ 6/98: IEEE S&P 98; Oakland no e-mail address available
o 5/12/98- 5/15/98: 10th CCSS, Ottawa; no e-mail address available
o 5/ 2/99- 5/ 5/99: IEEE S&P 99; Oakland no e-mail address available
o 5/11/99- 5/14/99: 11th CCSS, Ottawa; no e-mail address available
o 4/30/00- 5/ 3/00: IEEE S&P 00; Oakland no e-mail address available
o 5/16/00- 5/19/00: 12th CCSS, Ottawa; no e-mail address available

Key:

o ACISP = Australasian Conference on Information Security and Privacy, ACISP96
o ACSAC = Annual Computer Security Applications Conference

o ATMA = Advanced Transaction Models and Architectures ATMA
o BDBIS = Baltic Workshop on DB and IS, BDBIS
o CCS-3 = 3rd ACM Conference on Computer and Communications Security
o CCSS = Annual Canadian Computer Security Symposium
o CIKM = Int. Conf. on Information and Knowledge Management CIKM '95
o COMAD = Seventh Int'l Conference on Management of Data (India)
o CISMOD = International Conf. on Information Systems and Management of Data
o CFP = Conference on Computers, Freedom, and Privacy
o CoopIS96 = First IFCIS International Conference on Cooperative Information Systems, CoopIS96.
o COMPASS = Conference on Computer Assurance COMPASS'96
o CPAC = Cryptography - Policy and Algorithms Conference
o CRYPTO = IACR Annual CRYPTO Conference CRYPTO96
o CSFW = Computer Security Foundations Workshop CSFW96 and Wkshp page
o CWCP = Cambridge Workshop on Cryptographic Protocols
o DCCA = Dependable Computing for Critical Applications DCCA6
o DEXA = International Conference and Workshop on Database and Expert Systems Applications, DEXA96
o DMKD96 = Workshop on Research Issues on Data Mining and Knowledge Discovery,Web page and CFP.
o DOOD = Conference on Deductive and Object-Oriented Databases DOOD '95
o ESORICS = European Symposium on Research in Computer Security ESORICS'96
o FISP = Federal Internet Security Plan Workshop, FISP96.
o FISSEA = Federal Information Systems Security Educators' Association
o FME = Formal Methods Europe, FME '96
o FMSP = Formal Methods in Software Practice
o FSE = Fast Software Encryption
o HASE = High-Assurance Systems Engineering Workshop HASE96
o HPTS = Workshop on High Performance Transaction Systems
o IC3N = International Conference on Computer Communications and Networks
o ICDCS96 = The 16th International Conference on Distributed Computing Systems, ICDCS96
o ICDE = Int. Conf. on Data Engineering ICDE '95
o ICDT = International Conference on Database Theory ICDT97.
o ICI = International Cryptography Institute
o ICECCS = International Conference on Engineering of Complex Computer Systems
o ICSSDBM = Int. Conf. on Scientific and Statistical Database Management
o IEEE S&P = IEEE Symposium on Security and Privacy - IEEE S&P '96
o IFIP/SEC = International Conference on Information Security (IFIP TC11)

o IFIP WG11.3 = IFIP WG11.3 10th Working Conference on Database Security
o IFIP96 Mobile Commns = IFIP 1996 World Conference, Mobile Communications
o IH Workshop '96 = Workshop on Information Hiding
o IMACCC = IMA Conference on Cryptography and Coding, 5th IMACC
o IMC96 = IMC'96 Information Visualization and Mobile Computing
o INET = Internet Society Annual Conference
o INET96 = The Internet: Transforming Our Society Now, INET96
o IPIC = Integration of Enterprise Information and Processes, IPIC96
o IS = Information Systems (journal)
o ISTCS = Fourth Israeli Symposium on Theory of Computing and Systems, ISTCS96.
o IT-Sicherheit '95 = Communications and Multimedia Security: Joint Working conference of IFIP TC-6 and TC-11 and Austrian Computer Society
o IWES = International Workshop on Enterprise Security IWES
o JBCS = Journal of the Brazilian Computer Society
o JCMS = Journal of Computer Mediated Communication
o KDD96 = The Second International Conference on Knowledge Discovery and Data Mining (KDD-96)
o MCN = ACM Int. Conf. on Mobile Computing and Networking. See MOBICOM
o MCDA = Australian Workshop on Mobile Computing & Databases & Applications; MCDA96.
o MDS '95 = Second Conference on the Mathematics of Dependable Systems MDS-95
o METAD = First IEEE Metadata Conference METAD
o MMDMS = Wkshop on Multi-Media Database Management Systems MMDMS '96
o MOBICOM = Mobile Computing and Networking MOBICOM '96.
o NCSC = National Computer Security Conference
o NISS = National Information Systems Security Conference NISS96
o NSPW = New Security Paradigms Workshop
o OOER = Fourteenth Int. Conf. on Object-Oriented and Entity Relationship Modelling OOER '95
o PAKDD = First Asia-Pacific Conference on Knowledge Discovery and Data Mining, PAKDD97
o RBAC'95 = First ACM Workshop on Role-Based Access Control
o RTDB'96 = First International Workshop on Real-Time Databases: Issues and Applications, RTDB96.
o SAC = Workshop on Selected Areas of Cryptography SAC '96
o SCRAPC = Smart Card Research and Advanced Application Conference SCRAPC96

o SDSP = UK/Australian International Symposium On DSP For Communication Systems SDSP '96
o SECURICOM = World Congress on the Security of Information Systems and Telecommunication, SECURICOM '96
o SFTC-VI = Symposium on Fault Tolerant Computing - VI (Brazil)
o SIGMOD/PODS - ACM SIGMOD International Conference on Management of Data / ACM SIGACT SIGMOD-SIGART Symposium on Principles of Database Systems
o SNDSS = Symposium on Network and Distributed System Security (Internet Society) SNDSS '96
o SOC = 18th Biennial Symposium on Communiations, SOC18.
o TPHOLs = Theorem Proving in Higher Order Logics TPHOLs96
o TSMCFP96 = 4th International Conference on Telecommunication Systems
o USENIX Sec Symp = USENIX UNIX Security Symposium, 6th Annual.
o VLDB = 22nd International Conference on Very Large Data Bases, VLDB96.
o WDAG-9 = Ninth Int. Workshop on Distributed Algorithms
o WebNet = World Conference of the Web Society, WebNet96.
o WWWC = International World Wide Web Conference WWWC96.

Data Security Letter Subscription Offer

A special subscription rate of $25/year for the Data Security Letter is now available to IEEE TC members. The DSL is an external, nonpartisan newsletter published by Trusted Information Systems, Inc. Eleven issues (usually 16 pages each) per year are published. The DSL welcomes reader suggestions and contributions and accepts short research abstracts (about 130 words) for publication on an ongoing basis. On occasion, the DSL will be republishing Cipher articles (with authors' approval), but such articles will constitute a small portion of DSL content (thus there will be very little duplication of Cipher material).

IEEE TC members wishing to take advantage of the special subscription rate should send the following to sharon@tis.com. The information can also be faxed to 301-854-5363 (attention: DSL) phoned to 301-854-5338, or mailed to Trusted Information Systems, Inc., 3060 Washington Rd., Glenwood, MD 21738 USA.

NAME:

POSTAL ADDRESS:

(Please indicate company name, if a business address)

PHONE:
(Please indicate if home or business)

FAX:

E-MAIL:

IEEE Membership No. (if applicable):

NOTE: If you are already a paying subscriber to the DSL, for the $25 you will receive a 2-year renewal; refunds, rebates, etc., on your current subscription are not available.

If you have any questions about the offer or anything else pertaining to the DSL, you may contact the editor, Sharon Osuna, via E-Mail to sharon@tis.com or call her at 301-854-5338.

____

How to join the TC on Security and Privacy

____

You do NOT have to join either IEEE or the IEEE Computer Society to join the TC, and there is no cost to join the TC. All you need to do is fill out an application form and mail or fax it to the IEEE Computer Society. A copy of the form is included below (to simplify things, only the TC on Security and Privacy is included, and is marked for you) The full and complete form is available on the IEEE Computer Society's Web Server at URL: http://info.computer.org:80/tab/tcapplic.htm

PLEASE NOTE THAT THE FORM IS TO BE RETURNED (BY MAIL OR FAX) TO THE IEEE COMPUTER SOCIETY, >>NOT<< TO CIPHER.

---------

IEEE Computer Society
Technical Committee Membership Application

---

Please print clearly or type.

---

Last Name   First Name   Middle Initial

____

Company/Organization

____

Office Street Address (Please use street addresses over P.O.)

____

City State

____

Country Postal Code

____

Office Phone Fax

____

Email Address (Internet accessible)

____

Home Address (optional)

____

Home Phone

____

[ ] I am a member of the Computer Society

IMPORTANT: IEEE Member/Affiliate/Computer Society Number:

____

[ ] I am not a member of the Computer Society*

Please Note: In some TCs only current Computer Society members are eligible to receive Technical Committee newsletters.

Please select up to four Technical Committees/Technical Councils of interest.

TECHNICAL COMMITTEES

[X] T27 Security and Privacy

Please Return Form To:
IEEE Computer Society
1730 Massachusetts Ave, NW
Washington, DC 20036-1992
Phone: (202) 371-0101
FAX: (202) 728-9614

TC Publications for Sale

Just the thing for your valentine: proceedings from the 1995 IEEE Symposium on Security and Privacy, or for that touch of nostalgia order one of our past issues, available for purchase by TC members at favorable rates. Current issues in stock and continuing LOW PRICES are as follows:

	Price by mail		
	from TC	IEEE CS Press	IEEE CS Press
Year	TC members	IEEE member price	List Price
1992	$10	Only available from TC!	
1993	$15	Only available from TC!	
1994	$20	$30+$4 S&H	$60+$5 S&H
1995	$25	$25+$4 S&H	$50+$4 S&H

For overseas delivery:
-- by surface mail, please add $5 per order (3 volumes or fewer)
-- by air mail, please add $10 per volume
to the prices listed above.
If you would like to place an order, please send a letter specifying
which issues you would like,
 o where to send them, and
 o a check in US dollars, payable to the 1995 IEEE Symposium on
   Security and Privacy to:

Charles N. Payne
Treasurer, IEEE TC on Security and Privacy

Secure Computing Corp.
2675 Long Lake Rd.
Roseville, MN 55113

We remain unready to plunge our figurative toe into the inviting but potentially treacherous waters of electronic commerce!

TC Officer Roster

Chair:
Deborah Cooper
P.O. Box 17753
Arlington, VA 22216
(703)908-9312 voice and fax
dmcooper@ix.netcom.com

Vice Chair:
Charles P. Pfleeger
Trusted Information Systems, Inc.
3060 Washington Rd.,
Glenwood, MD 21738
(301)854-6889 (voice) (301)854-5363 (fax)
pfleeger@tis.com

Newsletter Editor:
Carl Landwehr
Code 5542
Naval Research Laboratory
Washington, DC 20375-5337
(202)767-3381
landwehr@itd.nrl.navy.mil

Chair, Subcommittee on Academic Affairs:
Prof. Karl Levitt
University of California, Davis
Division of Computer Science
Davis CA 95611
(916)752-0832
levitt@iris.ucdavis.edu

Standards Subcommittee Chair:
Greg Bergren
10528 Hunters Way
Laurel, MD 20723-5724
(410)684-7302
(410)684-7502 (fax)
glbergr@missi.ncsc.mil

Information for Subscribers and Contributors

SUBSCRIPTIONS: Two options:

1. To receive the full ascii CIPHER issues as e-mail, send e-mail to
   <cipher-request@itd.nrl.navy.mil>
   (which is NOT automated) with subject line "subscribe".

2. To receive a short e-mail note announcing when a new issue of CIPHER
   is available for Web browsing or downloading from our ftp server
   send e-mail to
   <cipher-request@itd.nrl.navy.mil>
   (which is NOT automated) with subject line "subscribe postcard".

To remove yourself from the subscription list, send e-mail to cipher-request@itd.nrl.navy.mil with subject line "unsubscribe".

Those with access to hypertext browsers may prefer to read Cipher that way. It can be found at URL
http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher

CONTRIBUTIONS: to <cipher@itd.nrl.navy.mil> are invited. Cipher is a NEWSletter, not a bulletin board or forum. It has a fixed set of departments, defined by the Table of Contents. Please indicate in the subject line for which department your contribution is intended. For Calendar entries, please include an e-mail address for the point-of-contact. ALL CONTRIBUTIONS CONSIDERED AS PERSONAL COMMENTS; USUAL DISCLAIMERS APPLY. All reuses of Cipher material should respect stated copyright notices, and should cite the sources explicitly; as a courtesy, publications using Cipher material should obtain permission from the contributors.

BACK ISSUES:
There is an archive that includes each copy distributed so far, in ascii, in files you can download at URL
http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-archive.html
There is also an anonymous FTP server that contains the same files.
To access the archive via anonymous FTP:

1. ftp www.itd.nrl.navy.mil
2. At prompt for ID, enter "anonymous"
3. At prompt for password, enter your actual, full e-mail address
4. Once you are logged in, change to the Cipher Directory:
   cd pub/cipher
5. Now you can request any of the files containing Cipher issues in ascii.
   Issues are named in the form: EI#N.9506 where N is the number of the
   issue desired and 9506 captures the year and month it first appeared.

=======end of Electronic Cipher Issue #12, 14 February 1996================